(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2002 (28.11.2002)

PCT

(10) International Publication Number
WO 02/095550 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IL02/00325

(22) International Filing Date: 24 April 2002 (24.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/286,403 25 April 2001 (25.04.2001) US

(71) Applicants and
(72) Inventors: **GREY, Marc, Elisha** [IL/IL]; Rashi St. 44, 63265 Tel-Aviv (IL). **BEN SHMUEL, Yohai** [IL/IL]; Rabbi Binyamin St. 6, 96163 Jerusalem (IL). **SINGER, Itay** [IL/IL]; Biet Zait 106, 90815 (IL). **BEN YOSEF, Amir** [IL/IL]; Lohamay Hagetaot St. 1, 49651 Petach Tikva (IL). **SHARON, Avner** [IL/IL]; Hahagana St. 4, 47203 Ramat Hasharon (IL). **YAGEL, Omer** [IL/IL]; Hasport St. 24, 34574 Haifa (IL).

(74) Agent: **NOAM, Meir**; P.O. Box 34335, 91342 Jerusalem (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/095550 A2

(54) Title: A SECURITY DEVICE USEFUL FOR PHYSICALLY SECURING DIGITAL DATA STORAGE MEDIA, AND A METHOD OF USE THEREOF

(57) Abstract: A security device, adapted for being coupled to a digital data storage media and to physically destroy said data in case of unauthorized using of the same is disclosed. This security device is comprises a physical destruction mechanism, enabling the physical destruction of said digital data storage media; protective means, protecting the said security device from unauthorized disarming; and an user user/computer interface, indicating unauthorized use of the said digital data storage media, and further to signal said distracting mechanism to district the digital data storage media following said use. A method for securing digital data storage media with a security device is also disclosed. Said method is comprising the steps of arming said security device; disabling said storage media: authorizing the use of said storage media, and in case of failing to supply said authorization, physically distorting said storage media.

A SECURITY DEVICE USEFUL FOR PHYSICALLY SECURING DIGITAL DATA STORAGE MEDIA, AND A METHOD OF USE THEREOF

FIELD OF THE INVENTION

The present invention relates generally to the field of digital data protection. More specifically, the present invention relates to a security device having means to physically securing digital data storage media, such as a computer hard drive. The present invention also relates to a method of use said device and to any electronic apparatus comprising the device.

BACKGROUND OF THE INVENTION

The security and protection of digitally stored information presents a major difficulty. This problem has only gotten greater as computer technology advances. Many security systems have been developed and implemented in order to permit authorized users to access computers and the data on hard drives, while preventing unauthorized users from operating the computer or retrieving data from the hard drive.

U.S. Patent No. 6,333,684 to Kang relates to a security device for a portable computer and method thereof. The invention provides a security device and a method for controlling the operating status of a portable computer using a pager, in order to prevent unauthorized access to information stored on the portable computer, in the event of a theft or a loss. The security device includes a memory for storing a pager processing routine, data processing means for receiving, storing, and determining pager information to generate an interrupt signal according to determined information, and a controller for displaying a message or a telephone number, or for changing a system password by performing a pager processing routine, according the interrupt signal from the data processing means. The security device disclosed in this invention is not 100% reliable since an unauthorized user could access and tamper with the pager processing routine. Also, the owner of the computer may not be aware that the portable computer has been

stolen, and thus will not activate the security device, and in the case the owner activates the security device, it offers a simple data protection that may be easily broken by an average hacker. Moreover, unauthorized user might access the magnetic media directly and read the data using suitable (and available) hardware & software.

U.S. Patent No. 5,872,515 to Ha et al. relates to a laptop computer with an anti-theft alarm function and a method of controlling the same. The laptop includes: a microcomputer both for controlling the LCD back-light section on/off operation in response to the on/off state of an LCD on/off switch and for generating an interrupt signal; an alarm processor for determining whether or not the interrupt signal is a burglar alarm signal and outputs an alarm in case of a robbery; and a password determining section for comparing a password entered by a user with a previously set password and interrupting the generation of an alarm only when both passwords are identical. A burglar alarm is sounded when an interrupt occurs so as to indicate a robbery as the LCD on/off switch is turned on against a user's will during the operation of the computer. The invention disclosed in this patent also does not meet the high security standards which are very often required, since, the alarm system could be readily manipulated or deactivated by an experienced computer hacker. This invention and many others that offer protection to the laptop (different alarms, cables, locks etc.) offer very little protection, if any, to the data. Those invention do not solve the problem of stilling the hard drive it self or the problem of reading the data after the computer is far from its owner.

U.S. Patent No. 6182223 to Rawson describes a method and apparatus for preventing unauthorized access to computer-stored information The invention includes a computer based security system to prevent unauthorized access to computer-stored information comprising several components. These are comprised of an intrusion detection mechanism, a ROM-based firmware program, an internal auxiliary power source, such as a battery sized to provide several minutes of operation of the computer system and all its internal devices, and a mechanism to reset the central processing unit of the computer and switch to a self contained power supply (i.e. battery power) responsive to the intrusion

detection mechanism. While providing a high level of security, the security system disclosed in this patent is also not always reliable. An unauthorized user could figure out a way to bypass the intrusion detection system. It is suggested that an unauthorized user could prevent the protection mechanism from operating the PC. Similarly, said unauthorized user might restored the data (in case a it was changed as a way of protecting it) by rendering any one of a handful of algorithms that amend hampered data or by interpreting the hysteretic remaining magnetic moments.

For certain private companies and many government agencies, an extremely high level of security is required to ensure that data does not end up in the wrong hands. This is especially the case with portable computing devices, which allow for the storage of gigabytes and even tetrabytes of information in a convenient and efficient manner. However, because of their easy mobility, they are very vulnerable to theft or misplacement. More often than not, the information stored on computers is of infinite more value than the computer itself. While the aforementioned patents are useful for providing a certain level of security, they do not provide a 100% guarantee that data will not be accessed and stolen. The information on the hard drive is still there, even once the various security mechanisms are actuated, and thus said data is still vulnerable to infiltration, no matter how highly sophisticated it's protection method is. The only way which would absolutely ensure that no unauthorized user gains access to information stored in a computer hard drive would be to equip the hard drive with a security device that would actually destroy the data-containing substrateof the hard drive when an unauthorized user tries to gain access to the information on the computer. This would ensure that highly confidential information does not end up in the wrong hands.

U.S. Pat. No. 6039637 to Hutchison et al. describes a security device for destroying the information bearing layer and data of a compact disc. The device includes a housing which has a first portion having an inner surface defining a first chamber. A second housing portion is selectively securable to the first housing portion to enclose the first

chamber. A mechanism is provided for selectively mounting a compact disc within the first chamber. An apparatus is disposed within the chamber for removing the information bearing surface from the substrate layer of a compact disc positioned on the mounting mechanism by physically converting the information bearing surface to particulate material. The removal apparatus is biased against the information-bearing surface of a compact disc positioned on the mounting mechanism as the information-bearing surface is reduced to particulate material. Finally, a mechanism is provided for selectively actuating the physical removal apparatus within the first chamber. While this invention provides a way to destroy the information on a CD, it does protect against instances where the CD is stolen or accessed by an unauthorized user. A security device is needed for digital data storage media that automatically and effectively destroys the data whenever an unauthorized user tries to access the data. The aforementioned invention is only useful when the user internationally uses the device to destroy the media. It is not useful in terms of active protection of the media against unauthorized users.

It is thus the primary object of the present invention to provide a method for protecting digital data that comprises effectively destroying the digital data if and when the data storage media ends up in the hands of an unauthorized user.
It is moreover an object of the present invention to provide a security device, adapted for being coupled to the storage media of the data, for effectively and physically destroying the digital data if and when an unauthorized user tries to access the data storage media.
It is still an object of the present invention to provide a security system which is activated wherein said computer has been taken away from it's owner by unauthorized identity.

It is additionally an object of the present invention to provide a security device and method that is 100% reliable and effective and leaves the owner of the media with no doubts as to whether or not confidential information has been improperly accessed.

These and other objects of the present invention will become more readily understood and appreciated from the summary of the invention and the detailed description of the drawings that follow.

SUMMARY OF THE INVENTION

It is thus the object of the present invention to provide a useful security device adapted for being coupled to a digital data storage media and to physically destroy said data in case of unauthorized using of the same. Said security device is comprising a physical destruction mechanism, enabling the physical destruction of said digital data storage media; a protective means, protecting the said security device from unauthorized disarming; and an user/computer interface, indicating unauthorized use of the said digital data storage media, and further to signal said distracting mechanism to distract the digital data storage media following said use.

The aforementioned digital data storage media are selected from a hard drive of a computer or one or more of its disks or any magnetic media comprising restorable data. More specifically, said computer is selected from desk computers and PCs, laptops, palms, cellular phones, memory units or any electronic apparatus comprises of digital data storage media.

According to one embodiment of the present invention, the destruction mechanism defined above is comprises an explosive element, or mechanical means selected from scratching, deforming, drilling, benting, breaking, or destroying the digital data storage media by means of mechanical spring; electro-magnetic motor; or piazo-electric motor.

According to one embodiment of the present invention, the destruction mechanism defined above is comprises chemical means, especially those that selected from acids, bases, oxidizing agents, radicals, solvents or any suitable component in gaseous, liquid or

solid states. Those chemicals are preferably having means to react, to form either exothermic or endothermic reaction adjacent to the digital data storage media, or alternatively, having means to destroy a significant portion of said storage media.

According another embodiment of the present invention, the said chemical means for destroying the digital data storage media comprises a capsule located within the security device and containing an acid solution. This capsule may comprise more then one compartment and a barrier is dividing said compartments, so when said barrier is destroyed, a chemical reaction is occur and the digital data storage media is destroyed.

It is thus in the scope of the present invention wherein those aforementioned means for destroying the digital data storage media or the capsule comprising the chemical means are thermodynamic or electromagnetic.

According to another embodiment of the present invention, said security device further comprising arming means coupled to said destroying means for activating the destroying means when an unauthorized user attempts to access data stored on said digital data storage media. Additionally, said device is comprising in another embodiment disarming means coupled to said destroying means for deactivating the destroying means when an authorized user attempts to access data stored on said digital data storage media. Said device is further comprising according another embodiment disabling means coupled to said destroying means for preventing access to data stored on said digital data storage media until said disarming means are activated.

It is in the scope of the present invention, wherein he said security device is comprises of triggering means coupled to said destroying means for enabling activating of said destroying means directly. Those triggering means are signal processing means, wherein said signal comprising a code; or alternatively encoded biological or physical parameters.

Another object of the present invention is to present useful electronic apparatus having a digital data storage media, comprising the security device as defined above.

Still another object of the present invention is to present useful method for securing digital data storage media with a the above defined security device, having means to enable the physical destruction of said digital data wherein said storage data or the device comprising the same is misused or used by unauthorized identity, comprising; (a) arming said security device; (b) disabling said storage media; (c) authorizing the use of said storage media; and in case of failing to supply said authorization, (d) physically distorting said storage media.

It is still acknowledged that the method defined above refers to digital data storage media stored in a computer, on a hard disk of a computer, and especially to a security device incorporated as part of the cover of the said hard drive. It is further acknowledged that the digital data storage data or the device comprising the same is misused or used by unauthorized identity is performed in the following cases selected from attempts to gain access to digital data storage media or to the said data by unauthorized user; attempts to remove said data form a location near its authorized owner or in cases the digital data storage media fail to sense a predetermined signal sent from its owner.

Lastly and more specifically, the present invention relates to a method comprising the steps of (a) activating arming via a code; (b) arming the security system; (c) disabling the hard disc; (d, 1) authorizing the user, by either supplying the security system an authorization code; disarming said security system; operating the hard disc of the computer; or alternatively (d, 2); failing to supply said authorization code and then physically distorting said hard disk.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 present a general scheme of the method for securing digital data storage media according to the present invention.

DETAILED DESCRIPTION OF THE DRAWING

According to the present invention, a security system useful for securing digital data contained on a hard drive of a computer is provided. This security system provides the owner of the computer 100% secure means in case said computer is undesirably used. The term 'digital data storage media' is referring hereto in the present invention particularly to a hard disk of a computer and especially to desk computers and PCs, laptops, palms, cellular phones, memory units or any electronic apparatus comprises of digital data storage media.

The following description is provided, along all chapters of the present invention, to enable any person skilled in the art to make use said invention and sets forth the best modes contemplated by the inventor of carrying out this invention. Various modifications, however, will remain apparent to those skilled in the art, since the generic principles of the present invention have been defined specifically to provide the said method for securing digital data stored on non volatile magnetic media.

The security system according to the present invention is gradually comprises of the following three components:

(i) destruction mechanism, enabling the destruction of the disk of the hard disk or any other ingredients of the computer gathering data to protect;

(ii)protective means designed to protect the said security system from unauthorized disarming; and

(iii) a user/computer interface, adapted to indicate undesirably use of the said computer and to signal the distracting mechanism to distract the computer is such cases.

It is acknowledged that both the said protective means and the user/computer interface may be referred to the term 'sensor', having means to activate the said destruction mechanism in cases of unauthorized and/or misuse of the computer. According to one embodiment of the invention, said sensor additionally comprising a comprising a control unit, having a ROM based firmware program and accessories, having *interalia* auxiliary source.

Destruction Mechanism

It is acknowledged that an effective destruction of the hard-drive is achieved wherein data recovery is proven to be practically and/or cost effective 100% unachievable Said effective destruction can be thus achieved by a few extreme precautions selected from smelting, disintegration, pulverization and incineration. Those radical solutions require professional intervention in the destruction process, as well designated equipment, i.e., metal destruction facilities, a shredding machine, etc. Additionally, application of an abrasive substance (i.e., emery wheel or disk sander) to a magnetic disk will achieve the same goal, while requiring human intervention

It is well acknowledged that when the hard drive device is operating it is essential that the surface of the disk will be smooth. According to the present invention, chemically active compounds are enabled to attack the surface of the disk, eradicate the lubrication and shielding layer, and attack the magnetic media.

In the context of the present invention, the term "effectively destroying" or "destroying" of digital data or a digital data storage media means any action, which damages or alters the storage media such that the data is practically gradually completely non-retrievable.

The term 'chemically active compounds' is referred in the present invention to components selected from, yet not limited to the group of acids, bases, oxidizing agents, radicals, solvents or any suitable component in gaseous, liquid or solid state having means to react with at least part of the hard disk, hard disk box or media, so the data gather on said hard disc is effectively destructed. It is further acknowledged that the term liquid is referring in the present invention for both waterborne and solvent base systems.

In one embodiment of the present invention, at least one hydrofluoric acid, hypochlorite hydrochloric, hydrofluoric, nitric acid or their mixture is used. In other embodiment of the present invention, raw materials are force to react to obtain an exothermic reaction so the hard disk is distract.

The amount of chemical that needs to be purged into the hard drive's shell in order to insure the eradication of the magnetic layer is proportional to the surface area of the interior of the hard drive's shell, assuming a layer thick enough to sustain the chemical reaction to completion.

The layers to be attacked are on the order of 100 nm thick. The interior surface of the hard drive, including the disk itself and various electronic components is about 200 square cm. It is thus why the required ensuing volume of said chemically active compounds are respectively low, and may be in the range of 1 ml or less to about 10 ml.

According to the present invention, said chemically active compounds are held in at least one capsule, made of glass, plastic or metallic materials. Once a signal coming from the control of the system is transmitted by wire or electromagnetic field, the said capsule is opened at least in its portion, so the chemically active compounds are allowed released towards the hard disk and distract it.

It is in the scope of the present invention wherein sad capsule comprising more then one compartment, wherein a barrier between said compartments is opened, raw materials are admixed and form an exothermic reaction, enabling the destruction of the hard disk. Thus, one best mode of said embodiment is wherein one compartment comprises of water and another compartments comprise of magnesium metal or potassium metal.

Further, the said barrier of both the unicompartment capsule or the multicompartment capsule is preferably comprising according the present invention shape memory materials, selected from Nitinol, poly-lactic acid or any other temperature, ultraviolet, ultrasonic depended matrices.

In order to spread the chemically active compound onto the disk entire surface, the capsule is potentially opened by braking or smashing it by a minute pyrotechnically means. Alternatively, various electronic means know in the art are possible and introduced in the present invention as a preferred embodiment.

According to the present invention, said smashing of either the disks of the hard disk or the capsule comprising the above defined chemically active compound is enabled by means of a pressure source having sufficient kinetic energy and mass to smash the said disks or capsule. Said pressure source is selected, yet not limited to scratching, deforming, drilling, benting or breaking the storage medium or any of the following: Mechanical spring; Electro-Magnetic motor; Piazo-Electric motor; or Magnetic motor.

It is well in the scope of the present invention, wherein aforementioned chemically active compounds are held in a plastic, glass or metallic capsule on top of the hard drive's shell. At the time said releasing is required, valves are opened, enabling the flow of said chemically active compounds into the hard drive.

When the heads read or write magnetic moments, they relay on their air bearing design and on elevation power to raise an average height of 0.25 μm above the disk surface. When not used, the heads are parked outside the data area of the disk. It is hence according another embodiment of the present invention to allow the press of the heads against the soft magnetic layer, thus physically and mechanically distracting the hard disk.

It is in the scope of the present invention to use sound waves of various frequencies as such as ultrasound, to create resonance will break a glass substrate disk.
One option well anchored in the present invention is distracting either the discs of the hard disk or the capsule comprising the chemical compounds by heat, wherein the heat source is selected from exothermic chemical reaction of a fuel material as defined above, or alternatively by means of endothermic reaction, causing the media to break due to increase brittleness and/or increased thermal stresses and/or changes of the molecular structure. Much similarly, said endothermic reaction is enabling the loose of data.

Protective Means

Protective means are designed according to the present invention to protect the aforementioned security system from unauthorized disarming.

A user/computer interface

Said interface is adapted to indicate undesirable use of the said computer, and as a result to signal the distracting mechanism to distract the computer is such cases. The pathway of the computer/user reciprocal encoding is comprising the following steps of activating the arming of the protective system by encoding the computer, or any auxiliary in

communication with the said computer, a predetermined code; disabling the hard disk so no data may be restored, aborted, copied, retrieved etc and then authorizing the user to use the computer and/or the data stored in it.

Said authorization is composed of two alternatives: either to *(i)* supply the security system the correct previously determined authorization code; disarming said security system; and then operating the hard disc of the computer; or alternatively *(ii)* failing to supply said authorization code and as a consequence, physically distorting said hard disc.

It is thus according to the present invention to provide a useful method to arm said protective system, and in particularly the destruction mechanism. The term 'armed' is referring in the present invention to a variety of scenarios and different levels of security. In one embodiment, the hard disk is armed every time the computer is turned off. Under such circumstances, when turned-on again the drive must be supplied with a an authorization signal. According to the presentinvention, the term authorization signal is referring tovarious authentication techniques i.e. biosensors; different techniques implemented to send a password, i.e. keyboard, radio/cellular; plugs i.e. smart card, plug. Those signalsare to be supplied to the drive to avoid its self-destruction. According to another embodiment, the hard disk is actively armed by sending it a signal or a special password.

According another embodiment of the present invention, the hard disk is also armed *via* mechanical means. Thus, attempts to tamper with the hard disk or remove it from its host computer would initiate its self-destruction.

It is acknowledged that the hard disk is provided with means for disabling the destruction. This can be done by means selected from (1) an electronic hardware key which must be plugged-into the drive or the host computer; (2) sending the drive a code via wireless transmitter/receiver combination; (3) employing some form of biometrics

authentication. Disarming the hard disk is not necessarily limited to a single code or a single step, but may include a series of operations and/or signals, which must be sent to the drive.

Immediately after supplying power to the disk drive, there is a need to prevent the normal operation of the drive, i.e. a need to prevent data from being read, until it is disarmed, and without causing irreversible damage to the drive. In one embodiment this disablement occurs when the free motion of the read/write arm of the drive is prevented. This is achieved simply by using a pin that prevents the arm from reaching the head. This pin is only raised once authentication takes place.

In another embodiment said disablement is achieved by using electromagnetic stopper and in a different embodiment the disc will not receive an electric current, unless it gets the user authentication. Authentication may be achieved in any number of ways, including but not limited to an electronic hardware key plugged-into the drive, sending the drive a code via wireless transmitter/receiver combination (preferred embodiment of authentication), or employing some form of biometrics authentication.

Besides the above-mentioned tampering, another embodiment of the present invention contemplates other events, which can initiate the drive to self-distract. Such destruction triggers would include (1) remote signal via wireless transmitter / receiver combination; (2) expiration (i.e. the drive has a fixed lifetime, after which it will self-destruct); and (3) inactivity – if the drive is not used for a specified amount of time, it will self-destruct, or alternatively, passive signal like being out of a set range from the user

The security system above defined has a rechargeable power source inside its system control. This source is obtaining power by pirating electricity from the hard drive, *via* the pins on the hard drive's ends. A small wire extension (an Electric Power Procurer) is

reaching from the system control to the hard drive power pins. As an alternative, the drive may be self-powered by an internal battery.

Referring to the system components above, the following is a description of how one embodiment of the invention is working. The description is intended to be an example implementation, which is subject to changes and other security enhancements to meet a variety of security needs.

In its initial state, the disk drive is armed. Before is used it must be disarmed, for instance by one of the means described above. In the event that this is successful the hard disk is operating normally. In the event that disarming fails to occur (usually indicative of a security breach) the drive is self-destructing *via* the predetermined mechanism. This destruction can also occur in response to other destruction triggers.

Reference is made now to Figure 1 presenting a method for physical securing of digital data storage media, and most specifically, the method for securing a hard disk of a computer, wherein said media coupled to said security device. According to one preferred embodiment of the present invention, the method of said physical securing is comprising the following steps: activating arming *via* a code (1); arming the security system (2); disabling the hard disc (3); and then authorizing the user, by either supplying the security system an authorization code: disarming said security system (4); and then operating the hard disc of the computer (5). Alternatively, failing to supply said authorization code by, also because of an external trigger (6) is follows by the final step of physically distorting said hard disk (7).

Reference is made to Figure 2, presenting a physical way according to the present invention to secure data storage from being used by unauthorised people, by mean of self-destruction mechanism. The data storage media, said a hard disk, is installed with the security system. In case of violation of media integrity, e.g. opening the hard disk case or in case that one decides to activate the device manually, or in case that the media is disconnected from its host (the computer) or in case that the media is connected to a non-authorized host computer, the explosive ring (100) is activated and destroys the magnetic media (90). The self-destruction mechanism is always alive. Using an internal power source (101) the system is kept alive and armed to its entire life. Once the main power supply is drained a secondary reservoir provide a single burst of power to activate the self-destruction mechanism and terminate the device.

According to one embodiment of the invention, once the host computer tries to boot the device, a user authentication process is generated. If authentication process fails, the control unit (102) overrides the device commands and prevents the reading heads (91) from accessing the media (90).

According to another embodiment of the invention, triggering of the self-destruction mechanism is enabled by at least one ways hereto defined: If an attempt to remove the cover from the media is made, a micro switch (103) is opened and informs the control unit (102) on the event. The control unit (102) than triggers the self-destruction mechanism and explodes the explosive ring (100). If a RF / Cellular / WLAN (e.g. Bluetooth, 802.11 etc.) / or any other electromagnetic transmission is received by the Antenna (104) and decoded into a self-destruct command by the control unit (102) the self-destruction mechanism is trigged and explodes the explosive ring (100). If the cover screws of the media's cover are unfastened, a magnetic flux sensor (105) senses the flux change and informs the control unit (102) on the event. The control unit (102) than triggers the self-destruction mechanism and explodes the explosive ring (100). If the cover is removed light enters the disk media enclosed chamber. A light sensor (106) than informs the control unit (102) on the event. The control unit (102) triggers the self-destruction mechanism and explodes the explosive ring (100). If the media is being investigated for its internal organization by X-ray, Gamma radiation or any other form on radiation, a radiation sensor (106) informs the control unit (102) on the event. The control unit (102) triggers the self-destruction mechanism and

explodes the explosive ring (100). If the cover screws of the media's cover are unfastened, an electronic circuit (107) is broken open and informs the control unit (102) on the event. The control unit (102) than triggers the self-destruction mechanism and explodes the explosive ring (100). If an attempt to remove the cover from the media is made, a magnetic coupling micro switch (108) is opened and informs the control unit (102) on the event. The control unit (102) than triggers the self-destruction mechanism and explodes the explosive ring (100). If an attempt to remove the cover from the media is made, an electromagnetic coupling micro switch (109), which is placed on the media hinge, or elsewhere with in the chamber, is opened and informs the control unit (102) on the event. The control unit (102) than triggers the self-destruction mechanism and explodes the explosive ring (100). If the media's cover is subjected to excessive force, *exampli gratia*, such as that which produced by a drilling tool, the strain gauges (110) change resistance and break open a circuit. The control unit (102) than checks for the strain pattern and decides whether or not to trigger the self-destruction mechanism and explodes the explosive ring (100). If the External triggering switch (111) is set to "on", the event is notified immediately to the control unit (102), and upon authentication it triggers the self destruction mechanism and explodes the explosive ring (100). If the media's case integrity is physically damaged, e.g., a hole or a cut through, any of the internal trip wires (112) is broken and informs on the event to the control unit (102). The control unit (102) than triggers the self-destruction mechanism and explodes the explosive ring (100). The trip wires may be materialized using wires impedance or by using piaso-electric sensors on the hoe of the cover's interior. If the media's case integrity is subjected to an extreme acceleration, a way over the device manufacturer original specifications, an acceleration sensor informs on the event to the control unit (102). The control unit (102) than triggers the self-destruction mechanism and explodes the explosive ring (100).

CLAIMS

1. A security device adapted for being coupled to a digital data storage media and to physically destroy said data in case of unauthorized using of the same, comprising;
   i. a physical destruction mechanism, enabling the physical destruction of said digital data storage media;
   ii. protective means, protecting the said security device from unauthorized disarming; and
   iii. an user/computer interface, indicating unauthorized use of the said digital data storage media, and further to signal said distracting mechanism to distract the digital data storage media following said use.

2. The system according to claim 1, wherein the digital data storage media is selected from a hard drive of a computer or one or more of its disks or any magnetic media comprising restorable data.

3. The system according to claim 2, wherein the computer is selected from desk computers and PCs, laptops, palms, cellular phones, memory units or any electronic apparatus comprises of digital data storage media.

4. A device according to claim 1, wherein the destruction mechanism comprises an explosive element.

5. The device according to claim 1, wherein the means for destroying the digital data storage media are mechanical.

6. The device according to claim 5, wherein the mechanical means are selected from scratching, deforming, drilling, benting, breaking, or destroying the digital data storage media by means of mechanical spring; electro-magnetic motor; or piazo-electric motor.

7. The device according to claim 1, wherein the means for destroying the digital data storage media are chemical.

8. The device according to claim 7, wherein the chemical means are selected from acids, bases, oxidizing agents, radicals, solvents or any suitable component in gaseous, liquid or solid states.

9. The device according to claim 7, wherein the chemical means are reacting to form either exothermic or endothermic reaction adjacent to the digital data storage media.

10. The device according to claim 7, wherein the chemical means are reacting with the digital data storage media, thus destroying significant portion of said media.

11. The device according to claim 1, wherein the means for destroying the digital data storage media comprises a capsule located within the security device and containing an acid solution.

12. The device according to claim 1, wherein the capsule comprising more then one compartment and a barrier is dividing said compartments, so when said barrier is destroyed, a chemical reaction is occur and the digital data storage media is destroyed.

13. The device according to claim 1, wherein the means for destroying the digital data storage media or the capsule comprising the chemical means are thermodynamic.

14. The device according to claim 1, wherein the means for destroying the digital data storage media or the capsule comprising the chemical means are electro-magnetic.

15. The device according to claim 1, further comprising arming means coupled to said destroying means for activating the destroying means when an unauthorized user attempts to access data stored on said digital data storage media.

16. The device according to claim 1, further comprising disarming means coupled to said destroying means for deactivating the destroying means when an authorized user attempts to access data stored on said digital data storage media.

17. The device according to claim 1, further comprising disabling means coupled to said destroying means for preventing access to data stored on said digital data storage media until said disarming means are activated.

18. The device according to claim 1, further comprising triggering means coupled to said destroying means for enabling activating of said destroying means directly.

19. The device according to claim 1, wherein the triggering means are signal processing, wherein said signal comprising a code.

20. The device according to claim 1, wherein the triggering means are signal processing, wherein said signal comprising biological or physical parameters.

21. Electronic apparatus having a digital data storage media, comprising the security device as defined in claim 1 or any of the preceding claim.

22. A method for securing digital data storage media with a security device as defined in claim 1 or any of the preceding claims, having means to enable the physical destruction of said digital data wherein said storage data or the device comprising the same is misused or used by unauthorized identity, comprising;

arming said security device;

disabling said storage media;

authorizing the use of said storage media;

and in case of failing to supply said authorization,

physically distorting said storage media.

23. The method according to claim 22, wherein the digital data storage media is stored in a computer.

24. The method according to claim 22, wherein the digital data storage media is stored in a hard disk of a computer.

25. The method according to claim 22, wherein the digital data storage data or the device comprising the same is misused or used by unauthorized identity is performed in the following cases selected from attempts to gain access to digital data storage media or to the said data by unauthorized user; attempts to remove said data form a location near its authorized owner or in cases the digital data storage media fail to sense a predetermined signal sent from its owner.

26. A method according to claim 22, wherein the security device is incorporated as part of the cover of the hard drive.

27. The method as defined in claim 22 comprising;

i. activating arming *via* a code;
ii. arming the security system;
iii. disabling the hard disc;
iv. authorizing the user, by either

supplying the security system an authorization code;
disarming said security system;
operating the hard disc of the computer;

or alternatively;

failing to supply said authorization code;
physically distorting said hard disk.

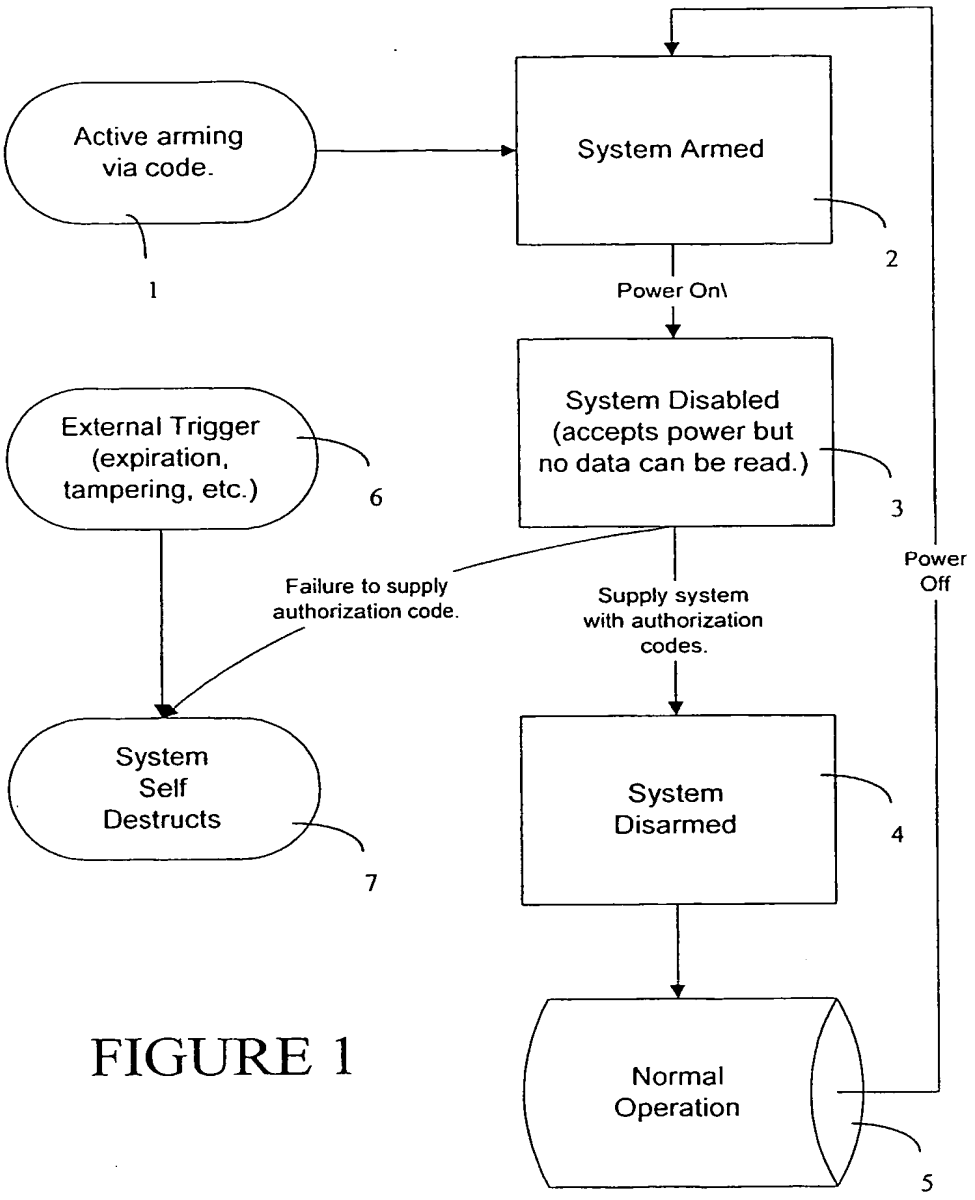

Active arming via code.
1
System Armed
2
Power On\
System Disabled (accepts power but no data can be read.)
3
External Trigger (expiration, tampering, etc.)
6
Failure to supply authorization code.
Supply system with authorization codes.
Power Off
System Self Destructs
7
System Disarmed
4
Normal Operation
5

FIGURE 1

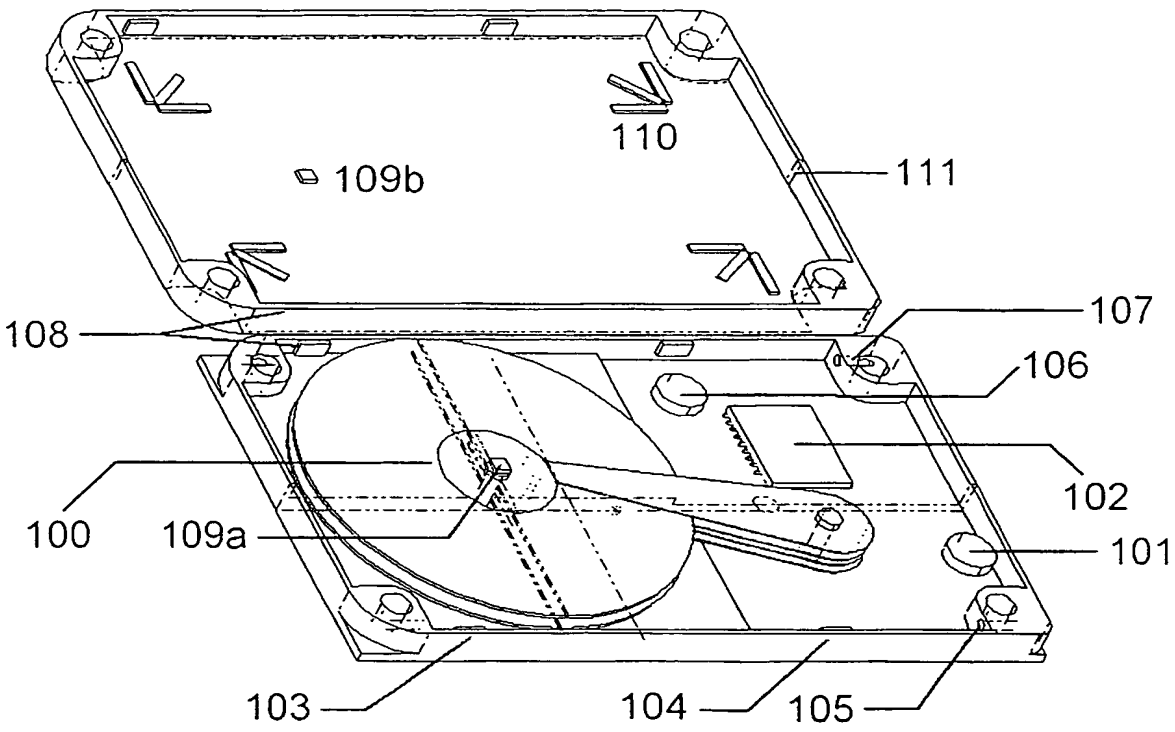


Figure 2

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 November 2002 (28.11.2002)

PCT

(10) International Publication Number
WO 02/095550 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IL02/00325

(22) International Filing Date: 24 April 2002 (24.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/286,403 25 April 2001 (25.04.2001) US

(71) Applicants and

(72) Inventors: **GREY, Marc, Elisha** [IL/IL]; Rashi St. 44, 63265 Tel-Aviv (IL). **BEN SHMUEL, Yohai** [IL/IL]; Rabbi Binyamin St. 6, 96163 Jerusalem (IL). **SINGER, Itay** [IL/IL]; Biet Zait 106, 90815 (IL). **BEN YOSEF, Amir** [IL/IL]; Lohamay Hagetaot St. 1, 49651 Petach Tikva (IL). **SHARON, Avner** [IL/IL]; Hahagana St. 4, 47203 Ramat Hasharon (IL). **YAGEL, Omer** [IL/IL]; Hasport St. 24, 34574 Haifa (IL).

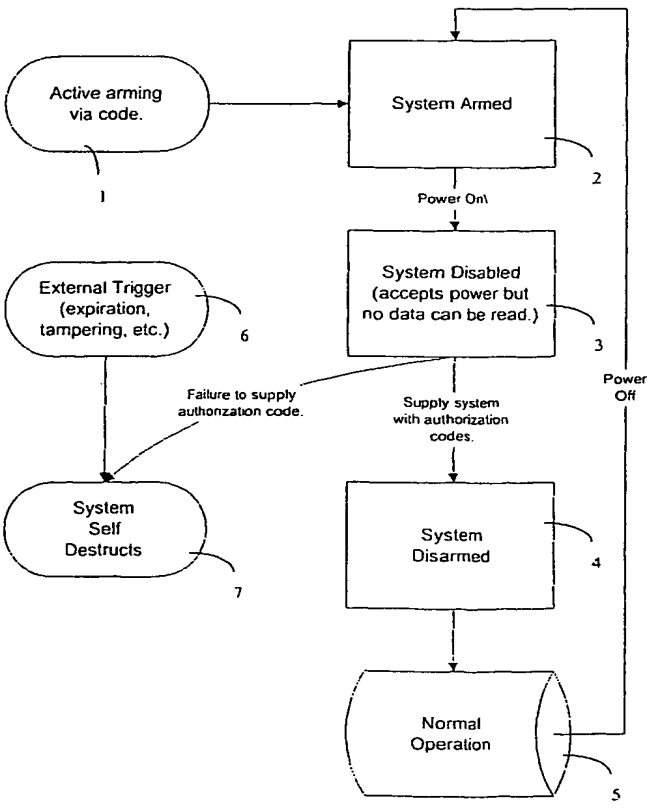
(74) Agent: NOAM, Meir; P.O. Box 34335, 91342 Jerusalem (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: A SECURITY DEVICE USEFUL FOR PHYSICALLY SECURING DIGITAL DATA STORAGE MEDIA, AND A METHOD OF USE THEREOF



(57) Abstract: A security device, adapted for being coupled to a digital data storage media and to physically destroy said data in case of unauthorized using of the same is disclosed. This security device comprises a physical destruction mechanism, enabling the physical destruction of said digital data storage media; protective means, protecting the said security device from unauthorized disarming; and an user user/computer interface, indicating unauthorized use of the said digital data storage media, and further to signal said distracting mechanism to district the digital data storage media following said use. A method for securing digital data storage media with a security device is also disclosed. Said method comprising the steps of arming said security device; disabling said storage media; authorizing the use of said storage media, and in case of failing to supply said authorization, physically distorting said storage media.

WO 02/095550 A3

Published:
— *with international search report*

(88) Date of publication of the international search report:
27 November 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00325

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 5 327 497 A (GLAZIER JAMES B ET AL) 5 July 1994 (1994-07-05) column 5, line 46 -column 6, line 13 column 7, line 18 - line 45; figures 5,7,8 ---	1-3,7-27 4-6
X Y	US 6 145 053 A (SMITH GORDON JAMES) 7 November 2000 (2000-11-07) abstract column 3, line 65 -column 4, line 28; figure 2 --- -/--	1-3, 15-19, 21-27 5,6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 August 2003	29/08/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 00453 A (TOBLER MARKUS ;HUG CARL (CH); KUTZLI JOERG (CH); EIDGENOESS MUNITI) 6 January 2000 (2000-01-06)	1-3, 21-24
Y	page 2, line 17 - line 28 page 8, line 20 -page 9, line 7 page 10, line 11 -page 11, line 11 page 16, line 26 -page 17, line 7; figures 1,5	4

INTERNATIONAL SEARCH REPORT

PCT/IL 02/00325

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5327497 A	05-07-1994	AU 681588 B2	04-09-1997
		AU 4528293 A	30-12-1993
		CA 2137274 A1	09-12-1993
		EP 0643858 A1	22-03-1995
		JP 7508604 T	21-09-1995
		WO 9324906 A1	09-12-1993
		US 5515440 A	07-05-1996
		US 5610981 A	11-03-1997
US 6145053 A	07-11-2000	CN 1329728 T	02-01-2002
		TW 455850 B	21-09-2001
		WO 0033191 A1	08-06-2000
WO 0000453 A	06-01-2000	EP 0968984 A1	05-01-2000
		AU 4255099 A	17-01-2000
		WO 0000453 A2	06-01-2000
		EP 1059275 A1	13-12-2000
		US 2001002297 A1	31-05-2001
		AT 238254 T	15-05-2003
		DE 59808071 D1	28-05-2003